(U) NCTS Guam EKMS Local Element Training

(U) EKMS User Security & Access Requirements

(U) Must have a security clearance equal to or higher than the highest classification of material issued to/or held by the User [EKMS-1B, article 414.d.1]

(U) SCI indoctrination is only required if material intended for use on SCI/SI circuits is issued to/used by the User [EKMS-1B, article 414.d.2]

(U) Must be authorized access to COMSEC material, in writing by the current Commanding Officer [EKMS-1B, article 414.d.3]

(U) Must execute and have on file a COMSEC Responsibility Acknowledgement Form (See Next Slide) [EKMS-1B, article 414.d.4 & NCTAMSPACINST 2280.2F, enclosure (3)]

ANNEX K COMSEC RESPONSIBILITY ACKNOWLEDGEMENT FORM

From:
(Rank/Rate, Full Name, SSN (Last 4), and Command of LE)

To: **EKMS Manager, NCTS GUAM**

Subj: **COMSEC RESPONSIBILITY ACKNOWLEDGEMENT**

Ref: (a) EKMS 1 (series)
(b) NAVCOMTELSTAGUAMINST 2280.1 (series)
(c) LOCAL ELEMENT COMMAND INSTRUCTIONS

1. I hereby acknowledge that I have read and understand refs (a-c).

2. I assume full responsibility for the proper handling, storage, inventorying, accounting, and disposition of the COMSEC material held in my custody and/or used by me.

3. I have been provided a copy of ref (a-c) or the location where an electronic version of current version of it is available by the EKMS Manager. If at any time I am in doubt as to the proper handling of COMSEC material that I am responsible for, I will immediately contact the EKMS Manager and request advice.

4. Before extended departure from the command (i.e., permanent transfer, or leave/TAD/TDY in excess of 30 days) I will report to the EKMS Manager and be relieved of responsibility for all COMSEC material that I have signed for.

SIGNATURE: _____

DATE: _____

Date relieved of COMSEC duties: _____

Destroy on/after date: _____
(90 days from the date relieved)

NOTES: 1. All personnel having access to or to whom COMSEC material is issued must complete a COMSEC Responsibility Acknowledgment Form. This requirement does not apply to individuals who access GPS key via the TAMPS for loading into aircraft.

2. This form will be reproduced locally and the required information will be typed or printed in black or blue-black ink. Retain in the Chronological File IAW Annex T.

3. The use of electronic signatures are acceptable provided all legal requirements (e.g., authenticity, non-repudiation, verification and records management/storage are met. Legal requirements include but are not limited to 15 U.S.C. 7001, 7006, and 7021.

(U) Two-Person Integrity (TPI) Handling/Storage

(U) Requires that at least two persons, authorized access to COMSEC keying material, be in constant view of each other and the COMSEC material requiring TPI whenever the material is accessed and handled. [EKMS-1B, article 510.a.1]

(U) Requires the use of an approved COMSEC vault or GSA approved security container. Must have GSA approved label on the outside. [EKMS-1B, article 510.a2]

(U) Will be equipped with a FF-L-2740/2740A or higher locking mechanism programmed w/ two different combinations to prevent single person access. [EKMS-1B, article 510.a.2]

(U) Storage at Shore Stations

(U) TS key in a COMSEC vault or GSA container. [EKMS-1B, article 520.c.1.a]

(U) S key in a COMSEC vault or in any security container approved for storing S or TS key. [EKMS-1B, article 520.c.1.b]

(U) C key in a file cabinet having a built-in three-position manipulation-resistant dial-type combination lock, or in any storage container approved for storing S or TS key. [EKMS-1B, article 520.c.1.c]

(U) Accountability Legend (AL) Codes

(U) AL-1: continuously accountable to the COR by accounting number from production to destruction. [EKMS-1B, article 230.a.1.a]

(U) AL-2: continuously accountable to the COR by quantity from production to destruction. [EKMS-1B, article 230.a.1.b]

(U) AL-4: locally accountable by quantity and handled/safeguarded based on classification. [EKMS-1B, article 230.a.1.c]

(U) AL-6: electronically generated and continuously accountable to the COR from production to destruction. [EKMS-1B, article 230.a.2.a]

(U) AL-7: electronically generated and locally accountable to the generating facility. [EKMS-1B, article 230.a.2.b]

(U) Inventories (Watch Station Environment)

(U) Watch Station: An occupied area which operates on a 24/7 basis in which responsibility for all COMSEC material is transferred from the off-going to the on-coming supervisor. [EKMS-1B, article 775.a]

(U) Custody: All COMSEC material held or used to a watch station must be reflected on and accounted for on a watch-to-watch (WTW) inventory. Local Element (LE) will maintain a local custody file containing the local custody document(s) (SF-153) for all material issued to the LE. [EKMS-1B, article 775.b]

(U) Responsibility: While on duty, each watch supervisor is responsible for all COMSEC material reflected on the WTW inventory, regardless of which watch supervisor signed the local custody document

(U) WTW Inventory Requirements

(U) All COMSEC material will be listed and inventoried by sighting the short title, edition, accounting number, and quantity. Equipment, which does not have an edition may be listed and inventoried by quantity only. [EKMS-1B, article 775.d.2]

(U) Must be dated and initialed or signed by individuals who conducted the inventory. [EKMS-1B, article 775.d.3]

(U) Conducted and witnessed by cleared and authorized personnel. [EKMS-1B, article 775.d.5]

(U) Returned items will be lined out and initialed (X2) on the WTW inventory. [EKMS-1B, article 775.d.6]

(U) Material not reflected on a WTW inventory (including incorrect accounting information), must be documented as a Practice Dangerous to Security (PDS) [EKMS-1B, article 775.d.7.note]

(U) Report WTW inventory discrepancies to the chain of command/EKMS Manager [EKMS-1B, article 775.f]

(U) Destruction

(U) Must be conducted by two properly cleared and authorized personnel [EKMS-1B, article 540.c]

(U) Destruction of key issued to a DTD/SKL does not require a CMS-25 unless otherwise directed [EKMS-1B, article 540.c.3.a]

(U) Destroy superseded key as soon as possible after the cryptoperiod and always within 12-hour after the end of the cryptoperiod [EKMS-1B, article 540.e]

(U) Only devices and methods approved by NSA, as reflected on the NSA Evaluated Products List (EPL) will be used for terminal destruction of COMSEC material [EKMS-1B, article 540.j.1]

CMS 25 Segmented Destruction Form for Use Locally

- Ensure that you use the correct CMS-25 for segmented destruction.
- Destruction/Extraction dates and time are to be written DTG format i.e. 211005ZAUG13
- Requires two (2) legible signatures for extraction and destruction.

CMS 25 (6) SEGMENT FORM

CMS-25 SUPERSESSION DESTRUCTION REPORT

THE INDIVIDUALS WHOSE SIGNATURES APPEAR BELOW, CERTIFY THAT THEY HAVE DESTROYED THE INDIVIDUAL KEYMAT SEGMENTS ON THE DATES INDICATED.

Segment/Card	Date Extracted	Date Destroyed	Destroyed By	Witness
1	230001ZAUG13	240001ZAUG13	SIGNATURE	SIGNATURE
2				
3				
4				
5				
6				

USS BACK YARD 259015
Command Title & Account Number

Short Title: **USKAT 1234** Edition: **MD** Reg Nr. **12359** ALC: **1**

EFFECTIVE: **23 AUG 2013** SUPERSEDED: **23 SEP 2013**

CONTROLLING AUTHORITY: **NCMS WASHINGTON D C**

C O N F I D E N T I A L (When Filled In)

Derived from: EKMS 1 (Series)
Declassify on: 22 SEP 2028

CMS 25 (MONTHLY) 30/31 DAY

CMS-25 SUPERSESSION DESTRUCTION REPORT

THE INDIVIDUALS WHOSE SIGNATURES APPEAR BELOW, CERTIFY THAT THEY HAVE DESTROYED THE INDIVIDUAL KEYMAT SEGMENTS ON THE DATES INDICATED.

Segment/Card	Date Extracted	Date Destroyed	Destroyed By	Witness
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				

_____
Command Title & Account Number

Short Title: _____ Edition: _____ Reg Nr. _____ ALC: _____

EFFECTIVE: _____ SUPERSEDED: _____

CONTROLLING AUTHORITY: _____

CONFIDENTIAL (When Filled In)

Derived from: EKMS 1 (Series)
Declassify on: 22 SEP 2028

Modern Key Log

- Required to maintain accountability of USFAU and circuits upon which it is loaded.
- Ensure that modern key is destroyed within 12 hours after verification that the circuit is operational.
- LOAD AND DESTROY!!!!!!

EXAMPLE OF MODERN KEY LOG

MODERN KEY MANAGEMENT LOG

COMMAND:

EQUIPMENT SERIAL #	KEY(S)	REG NUMBER	DATE LOADED(L) OR RE-KEYED(R) TO ECU	DATE EXPIRES	DATE ZEROIZED(Z) FM SKL/DTD	SIGNATURE
96357	USFAU 36989	21589642554	010001ZMAY2013	010001ZMAY2014	010200ZMAY13	SIGNATURE

LOCAL ELEMENT SPOTCHECKS

- The SCMSRO/CO may delegate two of the CO spot checks to the XO/ Communications Officer (COMMO), as long as the COMMO is not designated as the EKMS Manager or Alternate.
- Ensure that unannounced spot checks are conducted at least quarterly, of the COMSEC Vault and spaces where COMSEC material is used and stored.

LOCAL ELEMENT SPOTCHECKS cont.

- LE (Issuing or Using) Commanding Officers/OIC(s), including those in locations remote from the servicing or parent EKMS account, are responsible for conducting quarterly spot checks in accordance with Article 465 of EKMS 1 B Amendment 7.
- Servicing/parent EKMS accounts may require the reporting of spot check results; such a requirement should be spelled out in the LOA/MOU between the servicing command and the command being serviced.

LOCAL ELEMENT SPOTCHECKS cont.

- EKMS Managers and/or Alternates will conduct a minimum of one spot check per month **(minimum 12 per calendar year).**
- Additional spot checks by other senior, properly cleared chain of command personnel, i.e. COMMO, Operations Officer, Executive Officer, etc… are highly encouraged but at the discretion of the CO, ISIC or TYCOM.

(U) Practices Dangerous to Security (PDS)

(U//FOUO) Certain practices are not reported to the national level, but still have the potential to jeopardize the security of COMSEC material if allowed to perpetuate [NSTISSI 4003, annex C]

(U) All accounts must conduct annual PDS familiarization training [EKMS-1B, article 1001.b]

(U) Non-reportable PDS: discrepancy is not required to be reported outside the command but must be documented and reported to the CO [EKMS-1B, article 1001.d]

1. Late destruction, including key in a fill device, of COMSEC material (i.e., destruction not completed within the timeframes in this manual and superseded key received in a Reserve on Board (ROB) shipment from DCS (see Article 620.d) for this scenario), except where a waiver has been granted.

(U) Reportable PDSs include: premature or out-of-sequence use of key before its effective date as long as the material was not reused and inadvertent destruction when resupply is needed [EKMS-1B, articles 1005.b.1 and 1005.b.2]

(U) Report all PDS to the chain of command, EKMS Manager, and CO

(U) COMSEC Incidents

(U//FOUO) Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information or information governed by 10 U.S.C Section 2315 [NSTISSI 4003, paragraph 8.b]

(U) Disciplinary action should not be taken against individuals for reporting a COMSEC incident unless the incident occurred as a result of willful or gross neglect by those individuals [EKMS-1B, article 930.b]

(U) Any unit detecting a COMSEC incident will promptly report it per EKMS-1B, chapter nine. Reporting units do not have to be the unit that caused the incident. [EKMS-1B, article 940.a]

(U) COMSEC Incidents (Cont'd)

(U) Three types of COMSEC incidents: Cryptographic, Personnel, and Physical [EKMS-1B, article 905]

(U) Cryptographic: Use of compromised, superseded, or defective key [EKMS-1B, article 945.c]

(U) Personnel: Defection, espionage, or unauthorized disclosure of COMSEC material [EKMS-1B, article 945.d]

(U) Physical: Physical loss or compromise of COMSEC material, failure to review audit trail data, unauthorized access, material left unsecured, missing or non-use of local custody issue documentation, failure to maintain TPI for TS key, etc. [EKMS-1B, article 945.e]

(U) PDS/COMSEC Incident Prevention

(U) #1 Training/Awareness

(U//FOUO) #2 PDS and COMSEC incident reporting serve as the basis for identifying trends in occurrences and for developing procedural and doctrinal measures to prevent recurrence [NSTISSI 4003, paragraph 1]

(U) Questions